Building a Cybersecurity Program

A Tutorial for Managers and Pis

September 30th, 2013

Goal of this Training

Provide PIs and managers of NSF CI Projects with a basic understanding of risk-based cybersecurity programs, and guidance on managing their creation, evaluation and ongoing maintenance.

Outline

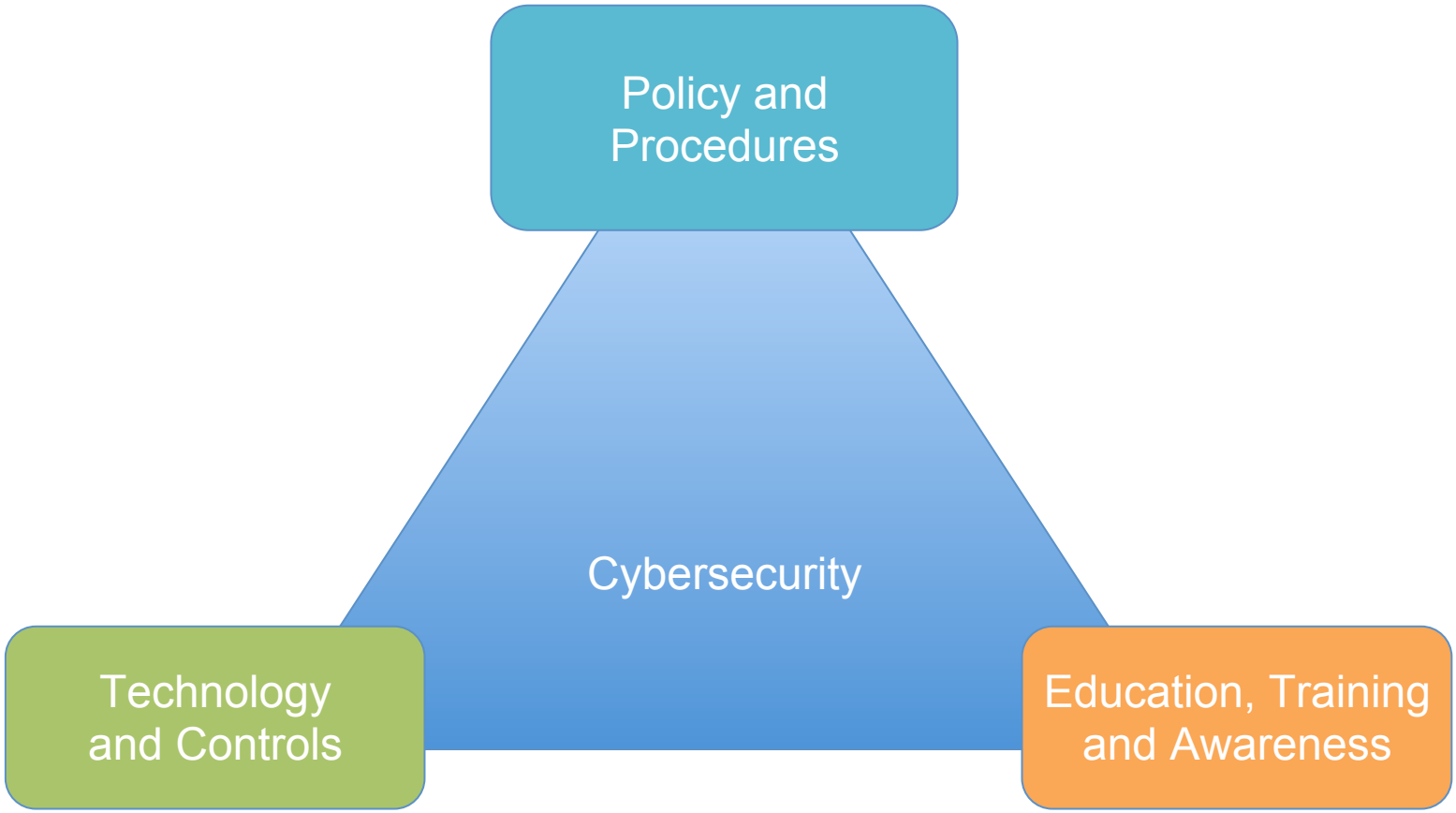
1. The benefits of and needs for a cybersecurity program.
2. Managing the creation and maintenance of a cybersecurity program that addresses your needs.
3. Basic cybersecurity plan components.
4. Risk management.
5. Case Study: CTSC Cybersecurity Program
6. How to evaluate a cybersecurity plan.
7. (Time allowing) Advanced cybersecurity program components.

BENEFITS OF AND NEEDS FOR A CYBERSECURITY PROGRAM

What is a Cybersecurity Program?

A ongoing process of managing information system risks through the use of policies, controls and education.

Key Components of a Cybersecurity Program



Why is a Cybersecurity Program for a NSF CI Project Needed?

Trustworthy Science

Maintaining the trust of scientists and the public in the CI, data and science.

A failure of CI that causes bad (or raises suspicion of) science results, and the resulting loss of trust by the community, would be the worst-case scenario.

Do no harm

CI represents some impressive cyber-facilities.

Being used as a tool to do harm to others would be potentially very damaging to a project's reputation.

Collaboration

CI is key to enabling collaborations by building trust between communities and people to allow for inter-organizational, inter-disciplinary collaboration.

Cybersecurity and trust is key to allowing collaborations and the inter-organizational, inter-disciplinary science they allow.

Minimize Disruption of Cyberattacks

Threats exist for any computers on the Internet, regardless of what it does.

Cybersecurity minimizes both the chance of those succeeding and the disruption if they do.

NSF Cooperative Agreements Information Security Requirement

Incorporated in NSF's Supplemental Financial and Administrative Terms and Conditions (next slide).

Purpose is to help ensure that NSF large facilities and FFRDCs have policies, procedures and practices to protect research and education activities in support of the award.

Influenced by recommendations from awardees at previous NSF-sponsored Cybersecurity Summits.

See CA-FATC LF Article 52 or CA-FATC FFRDC Article 55.

Information Security Responsibilities as listed in the Cooperative Agreement

Security for all IT systems is the Awardee's responsibility.

- Includes equipment, data and information.

Awardee is required to provide a summary of its IT Security program, including:

- Roles and responsibilities, risk assessment, technical safeguards, administrative safeguards; physical safeguards; policies and procedures; awareness and training; notification procedures.
- Evaluation criteria employed to assess the success of the program.

All sub-awardees, subcontractors, researchers and others with access to the awardee's systems and facilities shall have appropriate security measures in place.

Awardee will participate in ongoing dialog with NSF and others to promote awareness and sharing of best practices.

The facility itself is best able to assess cybersecurity appropriate for its operations.

MANAGING THE CREATION AND MAINTENANCE OF A CYBERSECURITY PROGRAM

Common Challenges

- Hard to dedicate cybersecurity staff in small projects.
- Lack of expertise/skilled staff - hard to find cybersecurity staff even if position exists.
- What is the best approach for my project? Where/how do I begin?
- Maintaining and refining an established Cybersecurity program.

Resource Management

What resources do you have in developing a Cybersecurity Program?

Project Staff

PI, researchers, students, partial funding of departmental support staff.

- Usually limited security expertise/ knowledge.

Leverage Institutional Resources

Departmental IT staff often have…

- Experience with administration and management of systems.
- Leverage existing policies and procedure (incident response, change management).

Leverage Campus Information Security Office

- Assistance with Risk Assessments.
- Security Training.
- Security Services (monitoring, firewalling, etc.)
- Forensic services.
- Knowledge of regulations FERPA, HIPAA.

Leverage NSF Community

- Experiences and practices of other CI projects.
  - http://trustedci.org/useful-links/
  - Ask them directly and build relationships.

- CTSC (trustedci.org)
  - Engagements and advice.
  - More about this tomorrow.

What is the best approach for my project? Where/how do I begin?

Some well-known frameworks:

- NIST 800-30 Rev 1
- ISO 27001
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

We recommend an approach based on these, but simplified and tailored for NSF projects.

Ideal Team to Develop a Cybersecurity Plan

A cybersecurity pro (or individual tasked to become one) who does bulk of the work.

Management - provides inputs on goals and acceptable risks, must support plan in practice.

Implementers/operations - provides input on cost and feasibility of controls.

What inputs does the planning process need?

Well-documented description of the project CI.

Understanding of tolerances of user/stakeholder with regards to security-versus-usability.

Management's goals and tolerance of risk.

Timeline for a Cybersecurity Plan

Planning can be scaled based on available time.

Quick and dirty focusing on obvious assets and threats with rudimentary policies and procedures.

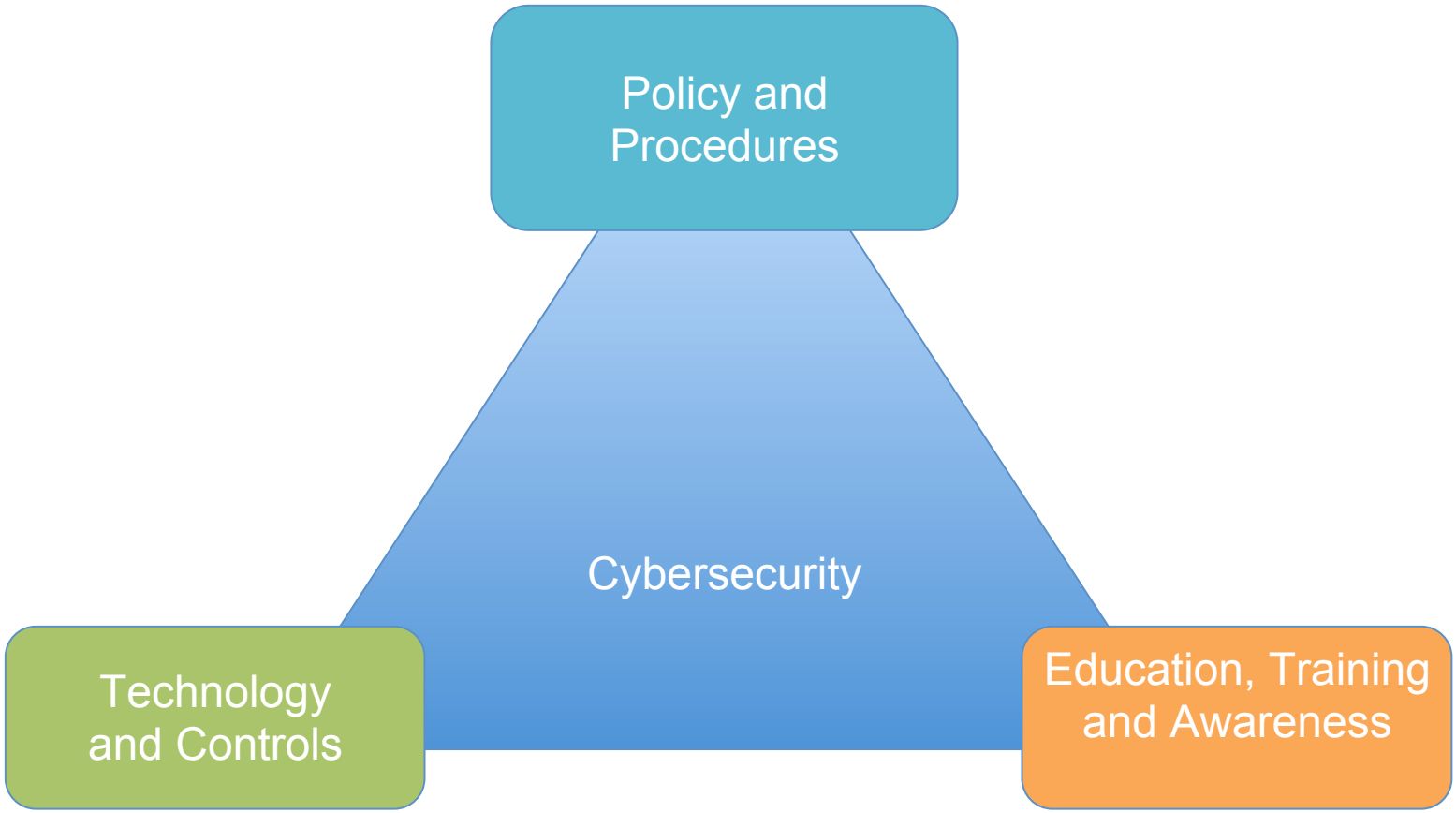
More time allows better identification of non-obvious assets, better planning for response, and more nuanced policies.

THE BASIC COMPONENTS OF A CYBERSECURITY PROGRAM

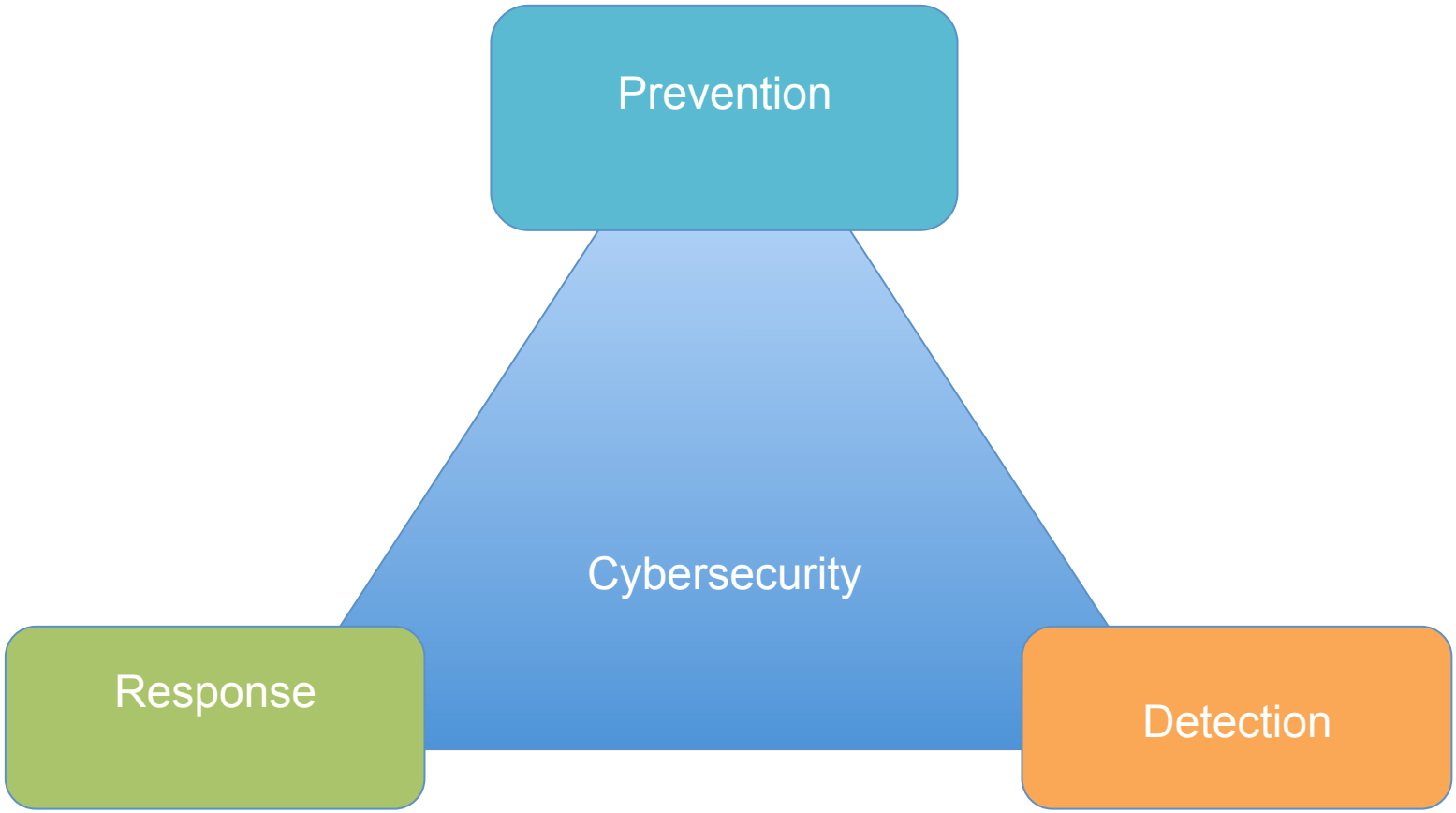
What is a Cybersecurity Program?

A ongoing process of managing risks through the use of policies, controls and education.

Key Components of a Cybersecurity Program



Component roles in a Cybersecurity Program



Prevention

"It's too late to sharpen your sword when the drum beats for battle."

Before the event, **preventive controls** are intended to prevent an incident from occurring, e.g. by keeping out unauthorized intruders.

Detection

During the event, **detective controls** are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police.

Work best in conjunction with preventative measures. When prevention fails, detection should kick in, preferably while there's still time to prevent damage. Includes log-keeping and auditing activities.

Response

After the event, **response** is intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

What Should a Basic Cybersecurity Program Cover?

1. Roles and responsibilities,
2. Risk assessment process,
3. Technical, administrative, and physical controls,
4. Policies and procedures,
5. Education, awareness and training,
6. Response and notifications in the event of a cyber-security breach,
7. Vulnerability identification.

Steps To Create a Cybersecurity Program

1. **Define roles and responsibilities**,
2. Have administrative, technical, and physical controls,
3. Have policies and procedures,
4. Perform regular risk assessment

Define Roles and Responsibilities

1. PI/Management:
    1. Promotes cybersecurity culture.
    2. Needs to sign off on acceptable level of risks.
    3. Needs to understand their role in implementing plan.
2. Security Officer/Security Team:
    1. Leads planning process and security-specific implementation.
    2. Training of staff.
3. Users:
    1. Needs to be trained to understand their role in plan.
    2. Must follow policies and procedures.

Roles and Responsibilities

PI/Management

- Be a Security Role Model.
- Protect the information you have been entrusted with,
- Understand the risks,
- Understand the, consequences
- Adhere and promote policy,
- Support your staff.

Security Officer/Team

You should have someone responsible for security day-to-day.

What do they do?

- Leadership,
- Monitoring,
- Enforcement,
- Direction,
- Security Policies & Standards,
- Awareness Training and Education,
- Respond/Investigate.

Security Officer/Team

Security Teams can be staffed by individuals across projects and departments. For example, team members could include resources outside of the funded CI staff:

- Departemental system administrators and network engineers.
- Campus information security personnel.
- Students and interns.

Steps To Create a Cybersecurity Program

1. Define roles and responsibilities,
2. **Have administrative, technical, and physical controls,**
3. Have policies and procedures,
4. Perform regular risk assessment

Security Controls

Controls are methods to help mitigate risk.

Controls can be administrative, technical, and physical.

Administrative Controls

Development and publishing of:

- Policies
- Standards
- Procedures
- Guidelines

Risk management activity.

Conducting and promoting security-awareness training.

Technical Controls

- Implementing and maintaining access control mechanisms,
- Password and resource management,
- Identification and authentication methods,
- Security devices,
- Configuration management of systems.

Physical Controls

- Controlling individual access into the facility and different departments,
- Accounting and logging of physical access to resources,
- Locking the systems and removing unnecessary media,
- Protecting the perimeter of the facility,
- Monitoring for intrusion,
- Environmental controls.

Steps To Create a Cybersecurity Program

1. Define roles and responsibilities,
2. Have administrative, technical, and physical controls,
3. **Have policies and procedures,**
4. Perform regular risk assessment

Policies and Procedures

1. Importance of writing down what you are doing.
2. For determining controls and education.
3. Sharing with others to build trust.
4. Data management policies so staff know how to handle user data.
5. Routine evaluation and updating.

Some Typical Policies and Procedures

Acceptable Use Policy

- What users are allowed to do on your CI.

Incident Response Plan

- How you respond when something goes wrong.
- Who to notify: locally, funding agencies, users.

Privacy Policy

- What you do with user's information.

Password Management Policy

- Allowable passwords, changing them.

Steps To Create a Cybersecurity Program

1. Define roles and responsibilities,
2. Have administrative, technical, and physical controls,
3. Have policies and procedures,
4. **Perform regular risk assessment**

RISK ASSESSMENT AND MANAGEMENT

Risk Management

Risk management refers to a coordinated set of activities to understand and respond to the many threats that can affect an organization's ability to achieve its objectives.

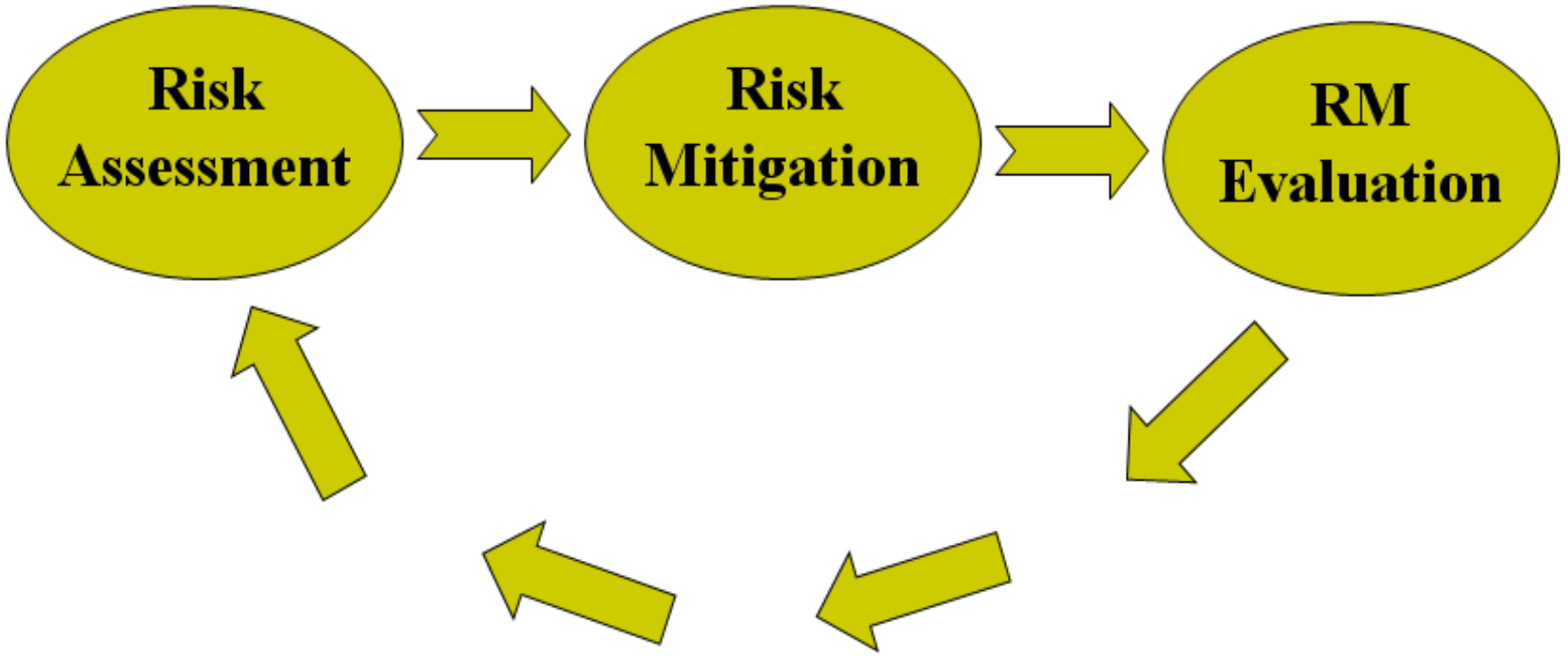
Ongoing risk management activities are typically a substantial component of a cybersecurity program.

Cybersecurity planning and programs are often components of broader risk management activities within an organization.

"Risk Management Dictionary". ISO 31000: http://www.praxiom.com/iso-31000-terms.htm

Risk Management

What is my risk? What will I do about it? How did I do?



NIST SP 800-30

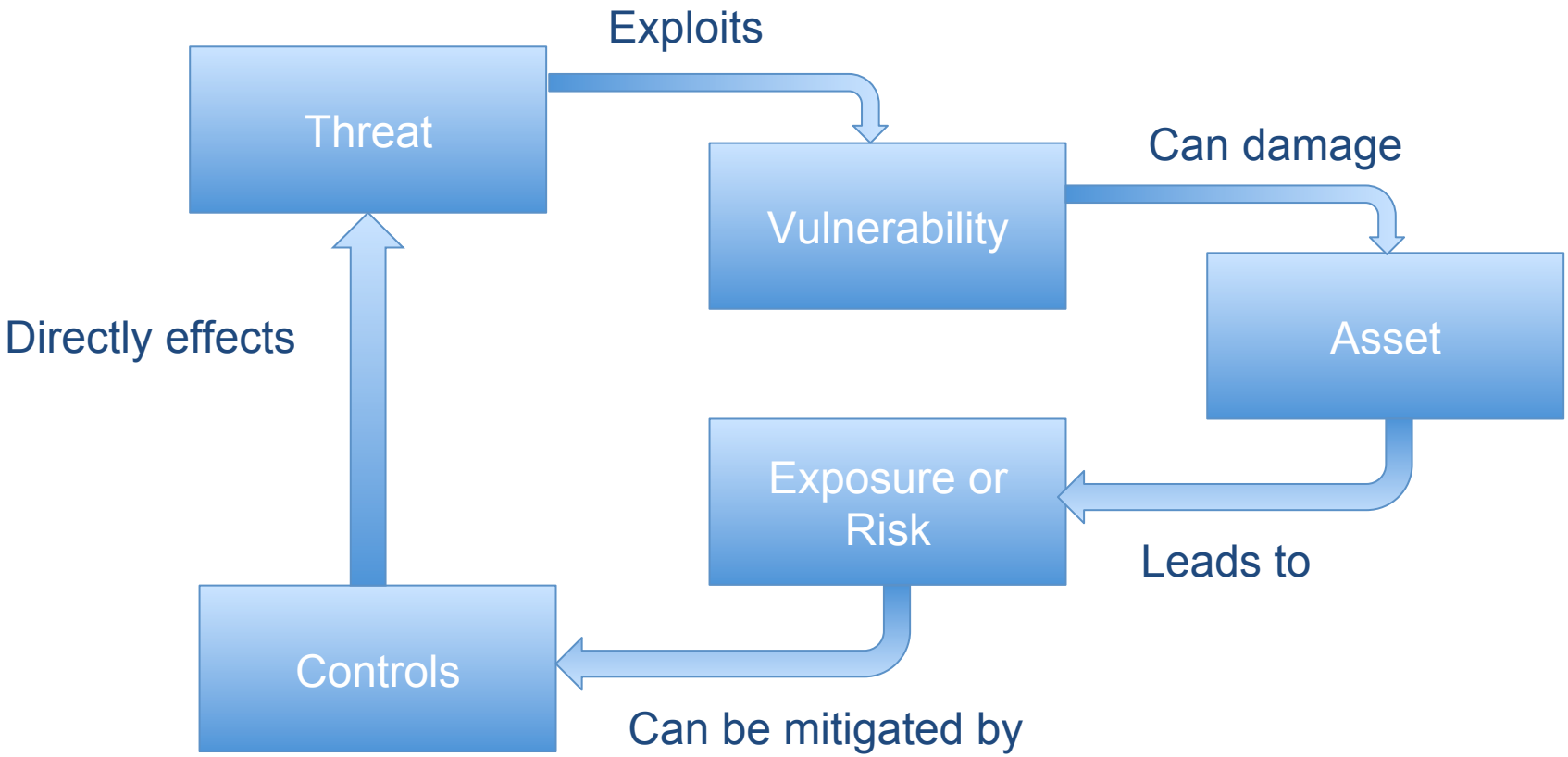
Risk Management at a High-Level

Assess: Assets, threats, vulnerabilities, and current controls. Gauge your risks based on likelihood and impact.

Mitigate: Document and implement recommended controls to manage risks.

Evaluate: Regularly assess how mitigations are doing, as well as how assets and risks are changing, and modify mitigations.

The Risk Cycle



Risk Management - Pros

Tailors a cybersecurity plan to fit unusual assets, specific project goals, and evolving threats.

Allows a project to quickly understand and adapt to changes.

Creates a strong, documented understanding of project, goals, and resulting plan.

Risk Management - Cons

Requires more effort than just following best practices, especially the first time.

Should be checked regularly (e.g. annually) for changes and updated to reflect changes.

Has subjective decision-making that requires judgment.

First Steps: Assess system, understand threats, vulnerabilities, and controls.

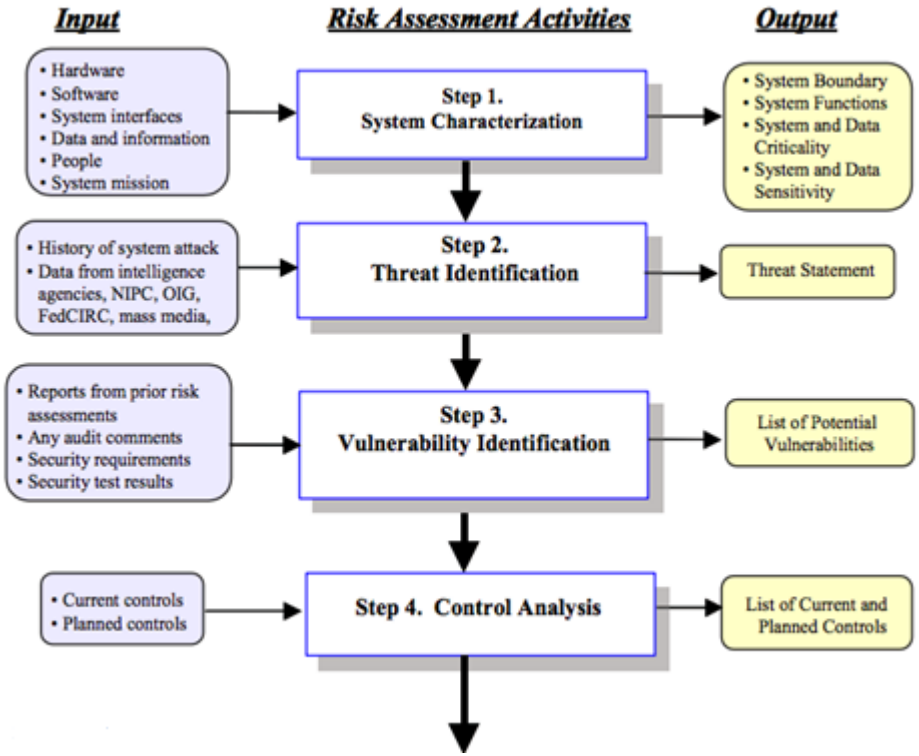
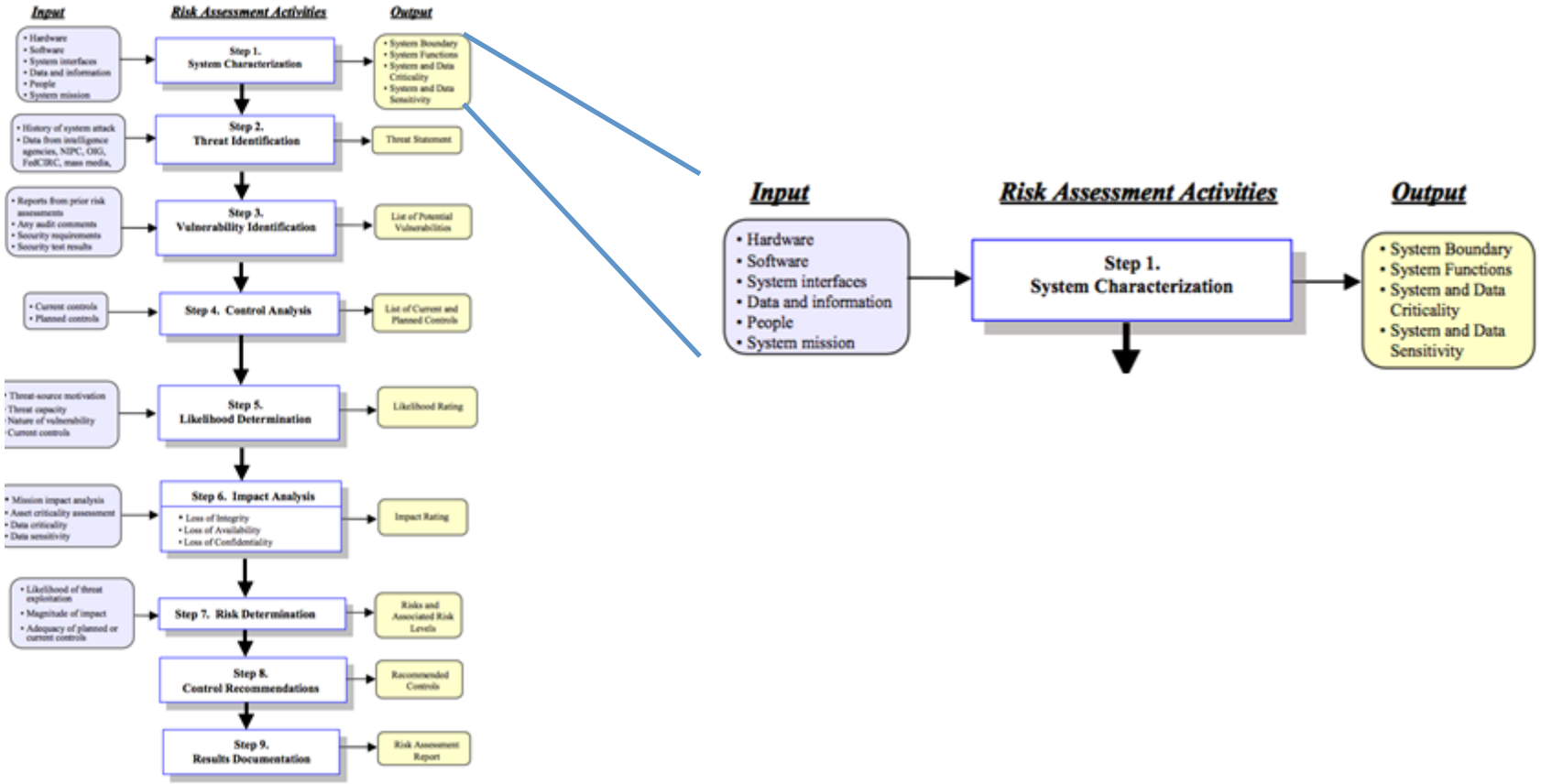


Image credit: NIST 800-30

Step 1: System Characterization



Assets

An asset is what we're trying to protect.

Things of value or sensitivity.

- Possibly systems, data, software, information.
- Can be intangible, e.g. reputation.
- Sensitive may not be valuable, e.g. personal information of users.

For each asset, understand it's importance and the concern: exposure, theft or unauthorized modification.

Asset Examples

More obvious:

- Pre-publication data (privacy, integrity)
- Systems and services
- Instruments
- Facilities
- Passwords, cryptographic keys, etc.
- Human subjects data

Less obvious:

- Public image / reputation – public web interfaces, twitter account, etc.
- Staff and user personal information
- User-supplied data
- Specialized software and analysis tools

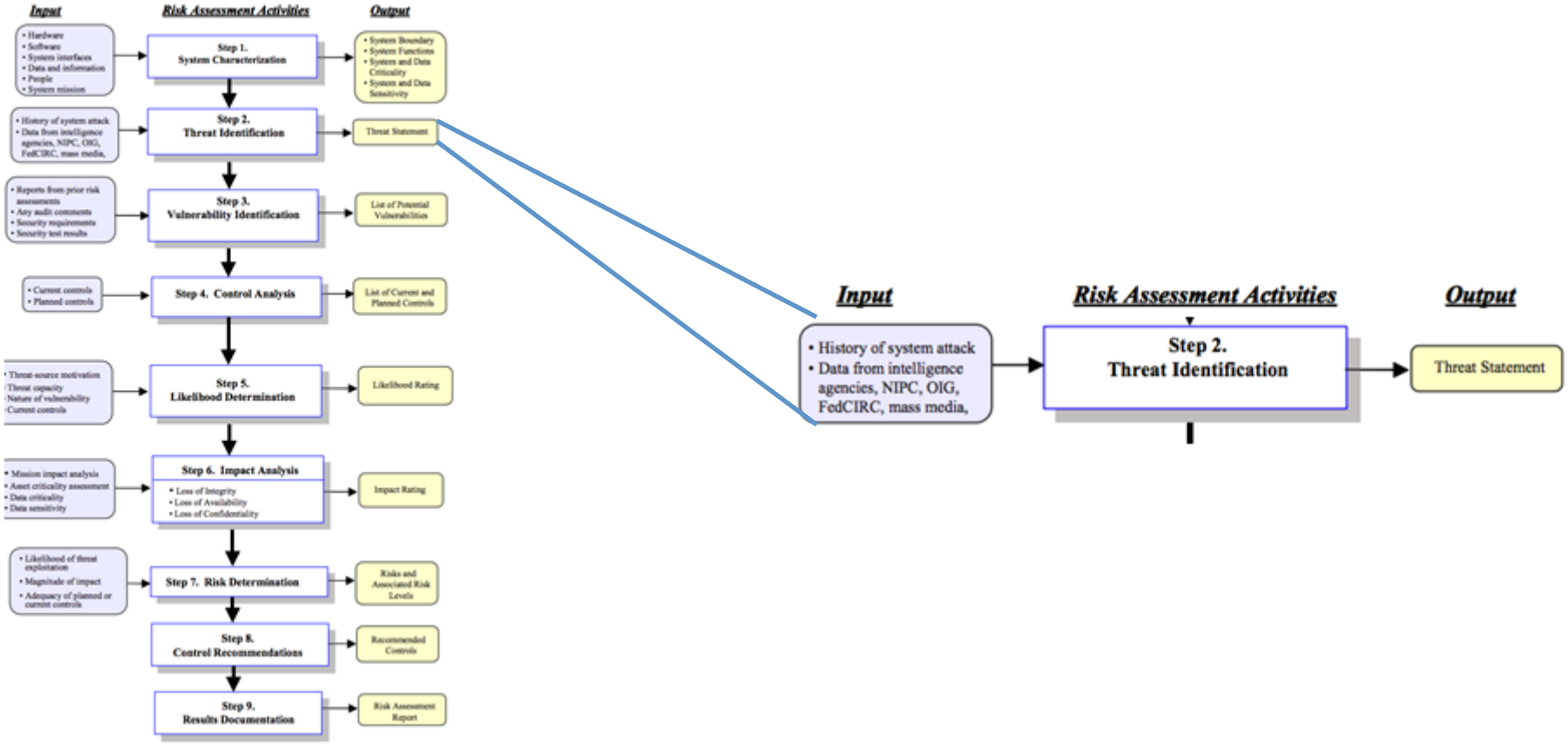
Attack Surfaces

How can the assets be accessed? Both intended and unintended interfaces.

These “attack surfaces” represent the system function and boundaries.

Some may be under your control, others not.

Step 2: Threat Identification



What is a Threat?

A **threat** is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy information or systems.

- Natural Threats
- Human Threats

A threat is what we're trying to protect against.

Threats: Actor, motivation, vector

Who, Why, How…

Understanding all three helps judge the likelihood and impact.

But I have nothing attackers care about...

A significant number of threats don't care who you are or what you are doing.

They want to use your computers to attack others, send SPAM, harvest passwords, serve porn, joy ride, brag, mine bitcoins, collect trophies…

Some common threat actors

Criminals

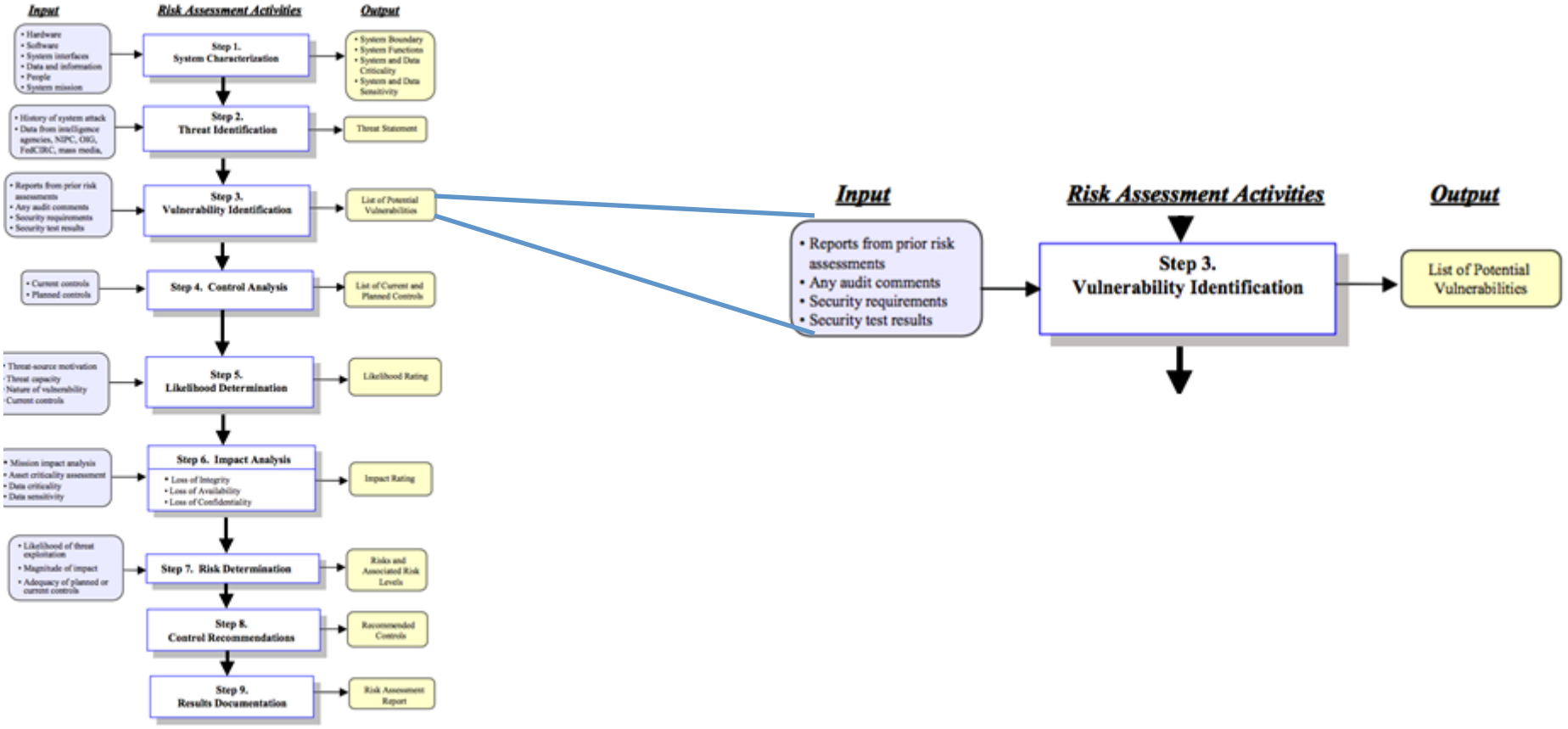
"Script kiddies"

Hacktivists

Insider threats
(misbehaving users or staff)

Joy riders, the curious, the trophy collectors and other hard to categorize individuals.

Step 3: Vulnerability Identification



Vulnerabilities

Weaknesses or gaps in a system that can be exploited by threats to gain unauthorized access to an asset.

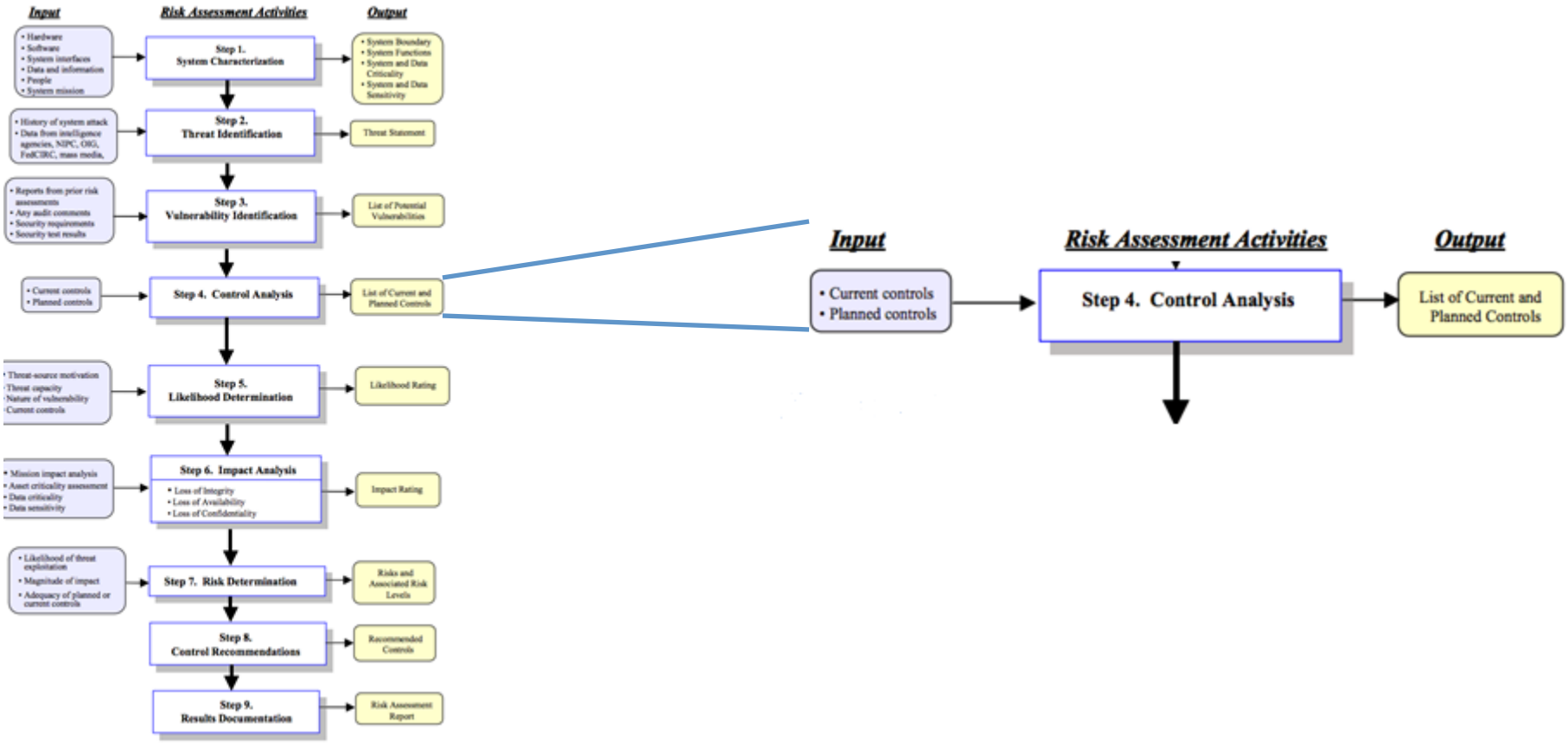
Can be identified by:

- Scanning,
- Assessment,
- Penetration testing,
- Known weaknesses/limitations in technology.

Example Vulnerabilities

- Passwords are known to be guessable and stealable from other sites.
- Unpatched system frozen for science run.
- Poorly administered systems.
- Web server assumed to have vulnerabilities.
- Old libraries needed for compatibility.
- "Zero-day" vulnerabilities that are not yet known.
- Humans are susceptible to social engineering.

Step 4: Control Analysis



Controls

A **control** is put into place to mitigate the potential risk.

Determine what controls are already in place.

Ideally from documentation from prior assessments, system plans, documented project policies.

If not documented, then by doing inventory and interviewing staff.

Example Controls

Physical controls:

- Controlling individual access into the facility and different departments
- Accounting and logging of physical access to resources
- Locking the systems and removing unnecessary media
- Protecting the perimeter of the facility
- Monitoring for intrusion
- Environmental controls

Technical controls:

- Implementing and maintaining access control mechanisms,
- Password and resource management,
- Identification and authentication methods,
- Security devices
- Configuration management of systems

Administrative controls:

Development and publishing of

- Policies
- Standards
- Procedures
- Guidelines

- Risk management activity
- Conducting and promoting security-awareness training

Next Steps: Assess Risks, document recommended controls.

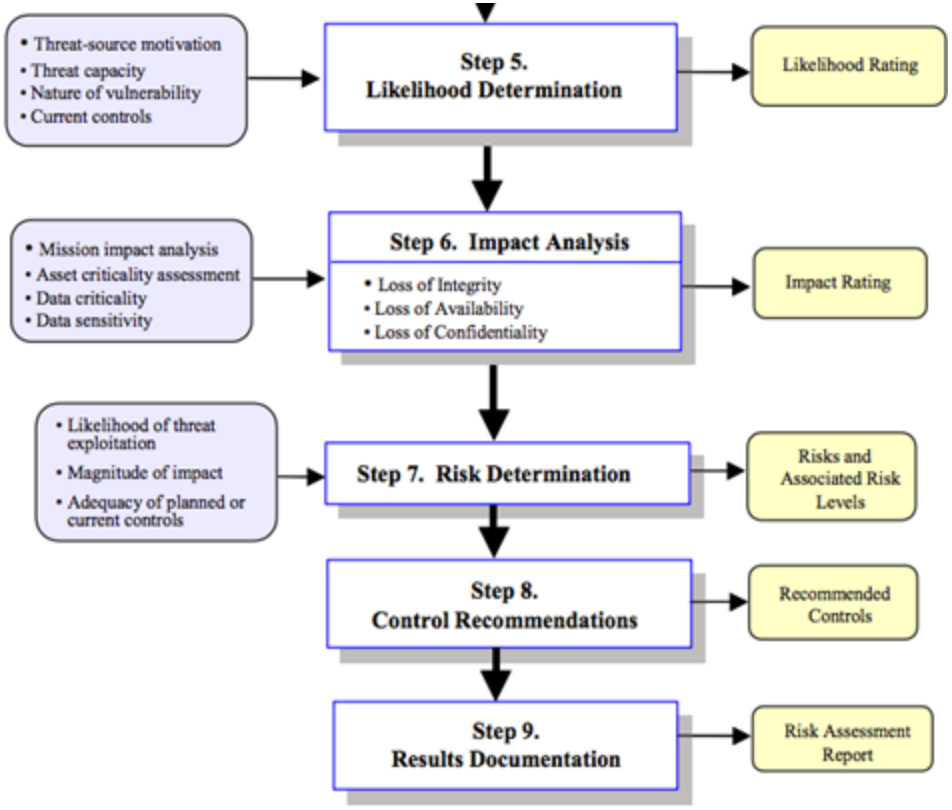
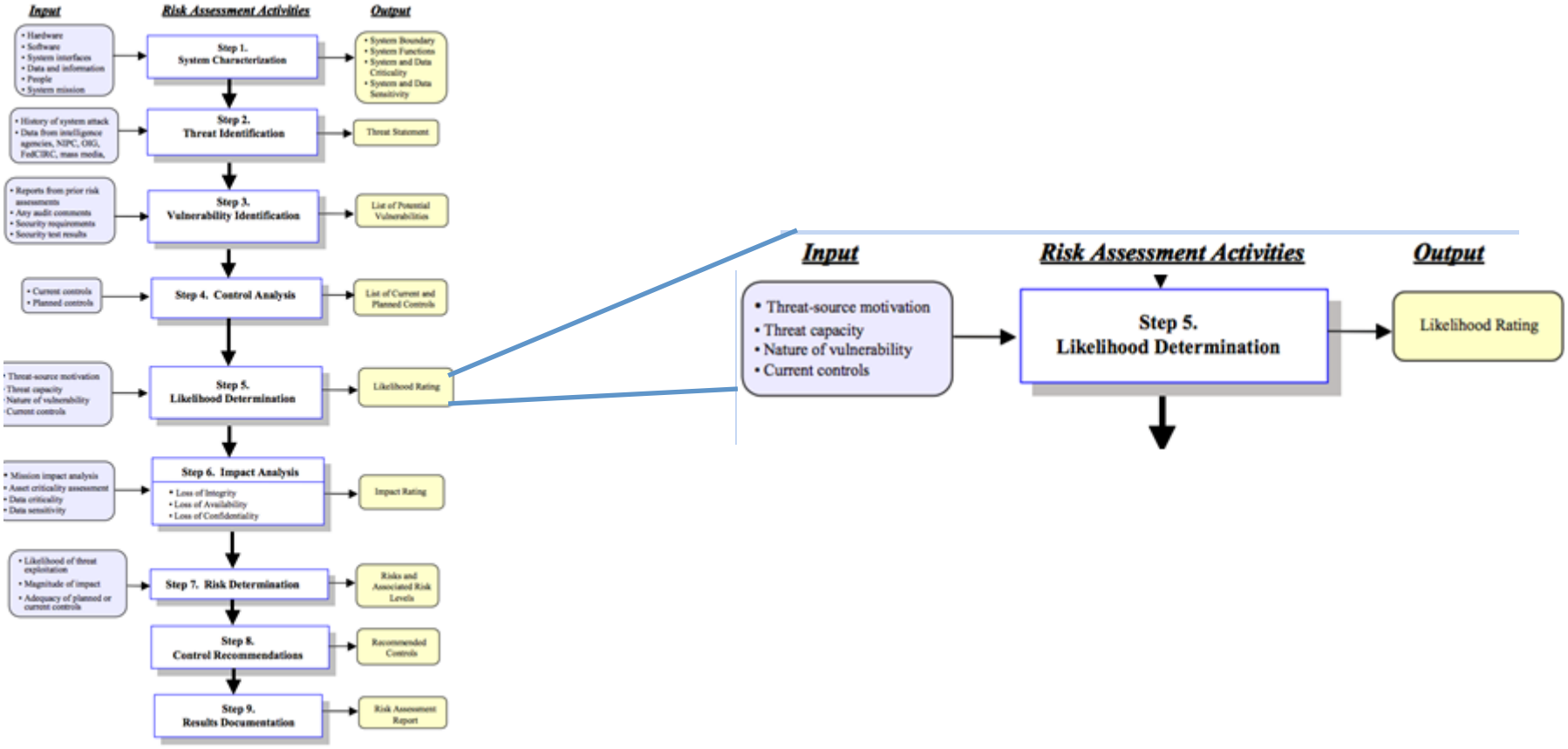


Image credit: NIST 800-30

Step 5: Likelihood Determination



How likely is it threat will be realized?

Likelihood is the probability that a vulnerability will be exercised by a threat.

Factors:

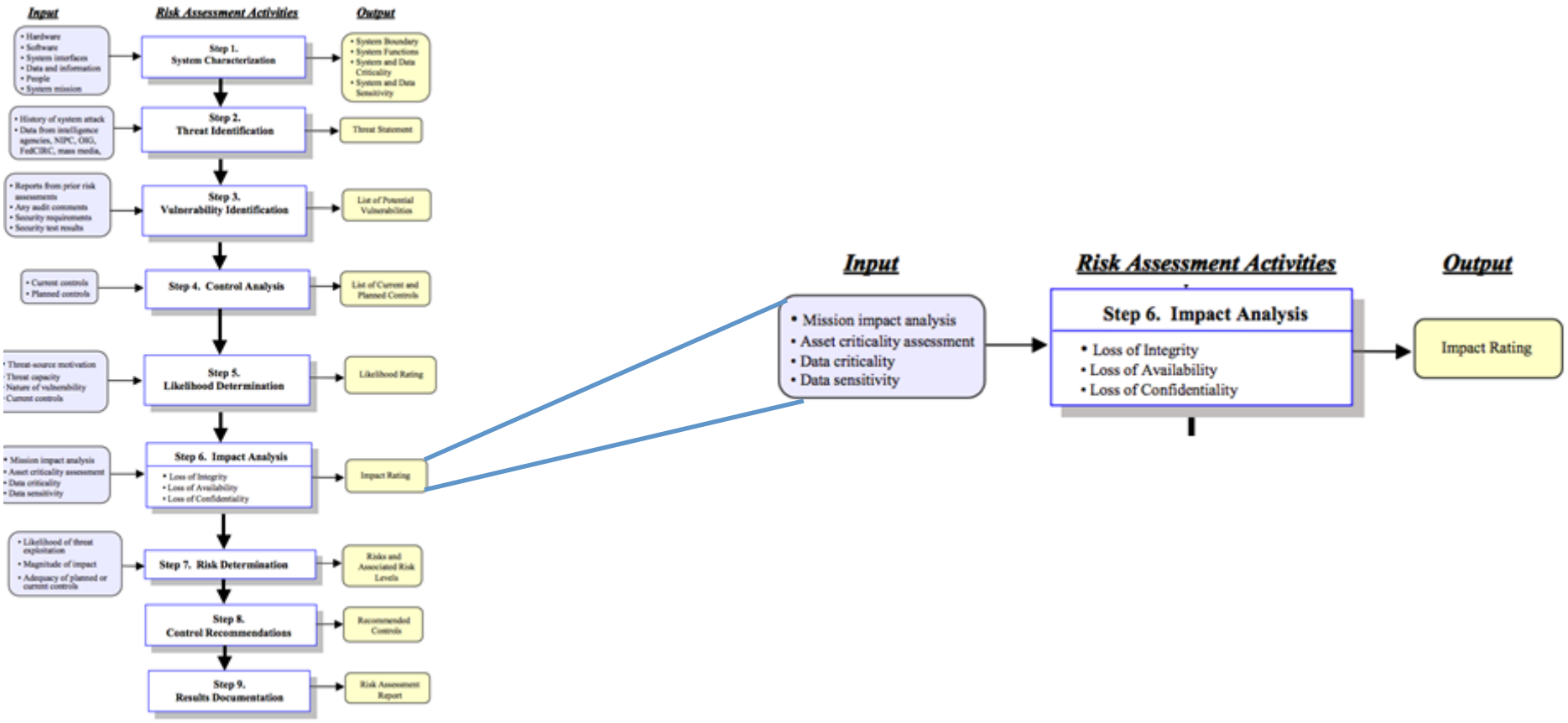
- Threat motivation and capability.
- Nature of the vulnerability.
- Existence and effectiveness of current controls.
- History.

Ranking of Likelihood

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

A coarse estimation is sufficient. There is a fair amount of guesswork involved in this estimation. Best not to get too hung up, estimate and re-evaluate over time. (Sharing of experiences helps a lot here.)

Step 6: Impact Analysis



What is the Impact?

Impact of a security event can be described in terms of loss or degradation of assets or services that impact project goals.

Impacts can be:

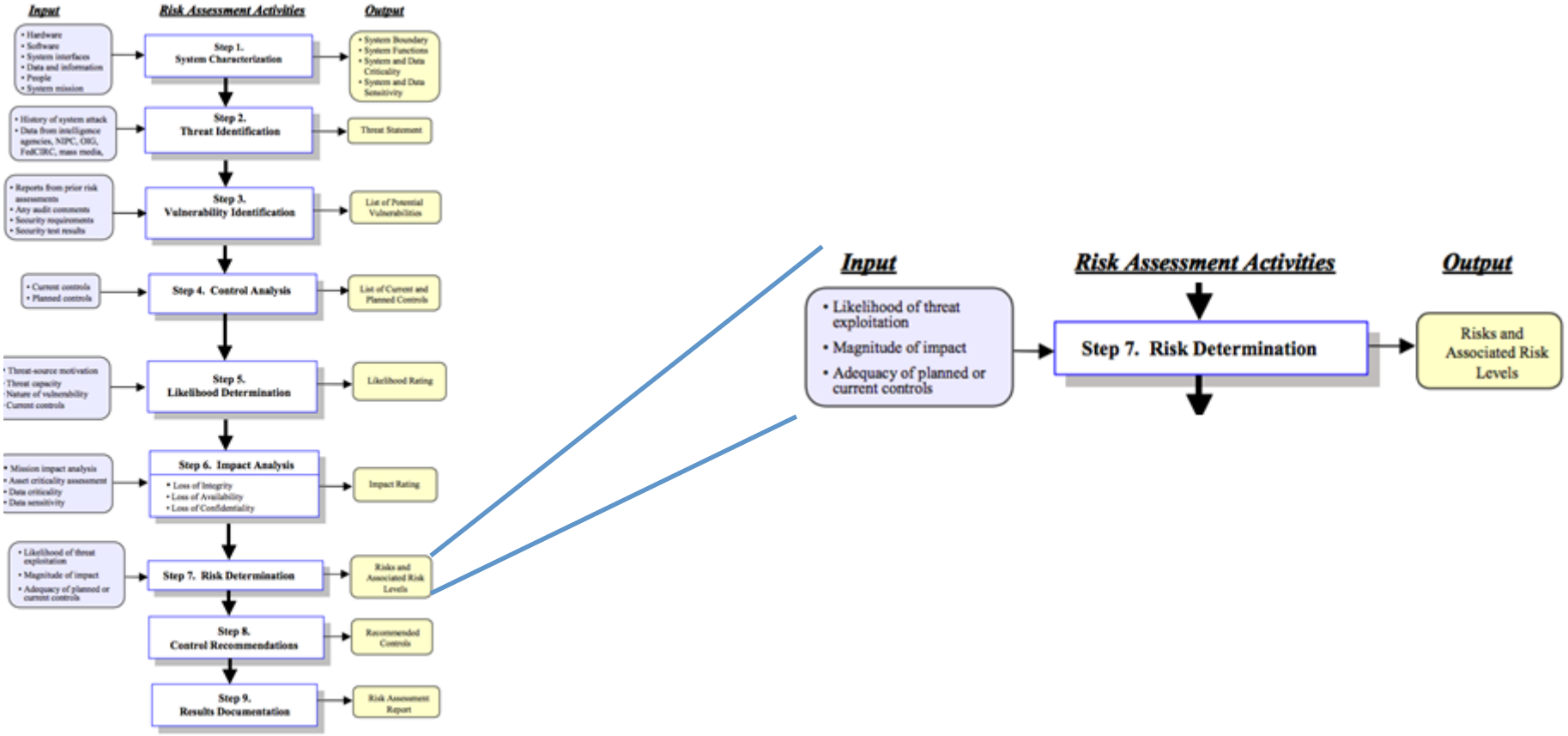
- Data exposure.
- Service unavailability.
- Embarrassment.
- Loss of users.
- Staff time spent recovering.
- Loss of trust by collaborators.

Rating of Impact

Magnitude of	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Again, a coarse estimation is sufficient. Understanding the projects goals and stakeholder expectations is important here.

Step 7: Risk Determination



Risk Formula

Yes, this is fuzzy math. All we are trying to do is estimate our risks and prioritize them.

Calculating Risk

Threat Likelihood	Impact		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

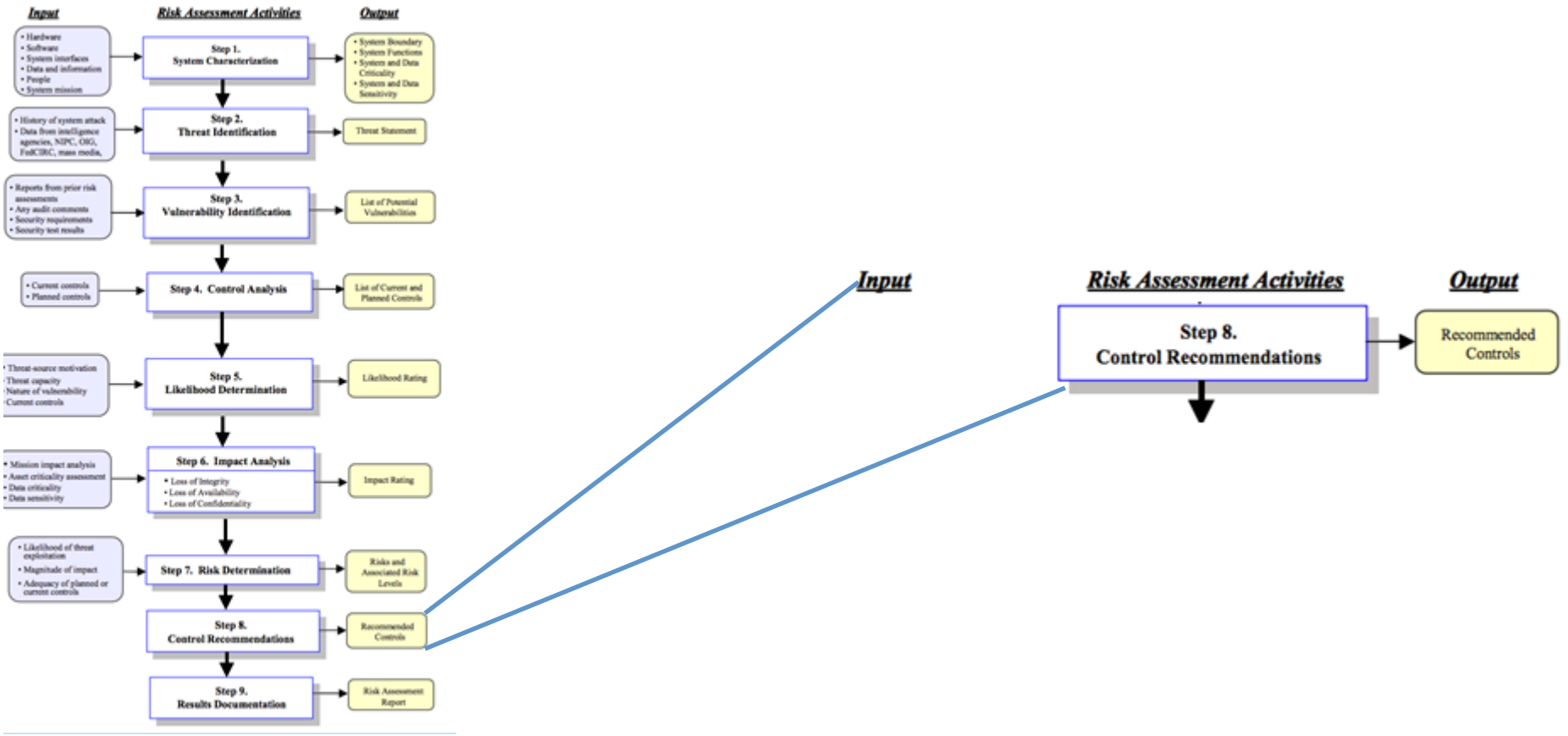
One can use numerical values to use a spreadsheet for calculating risk.
Don't read too much into the numbers though, they are just relative to prioritize the risks.

Rating of Risks

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk

Again, coarse values usually suffice. For lots of risks, you might want to be finer-grained to get more differentiation.

Step 8: Control Recommendations



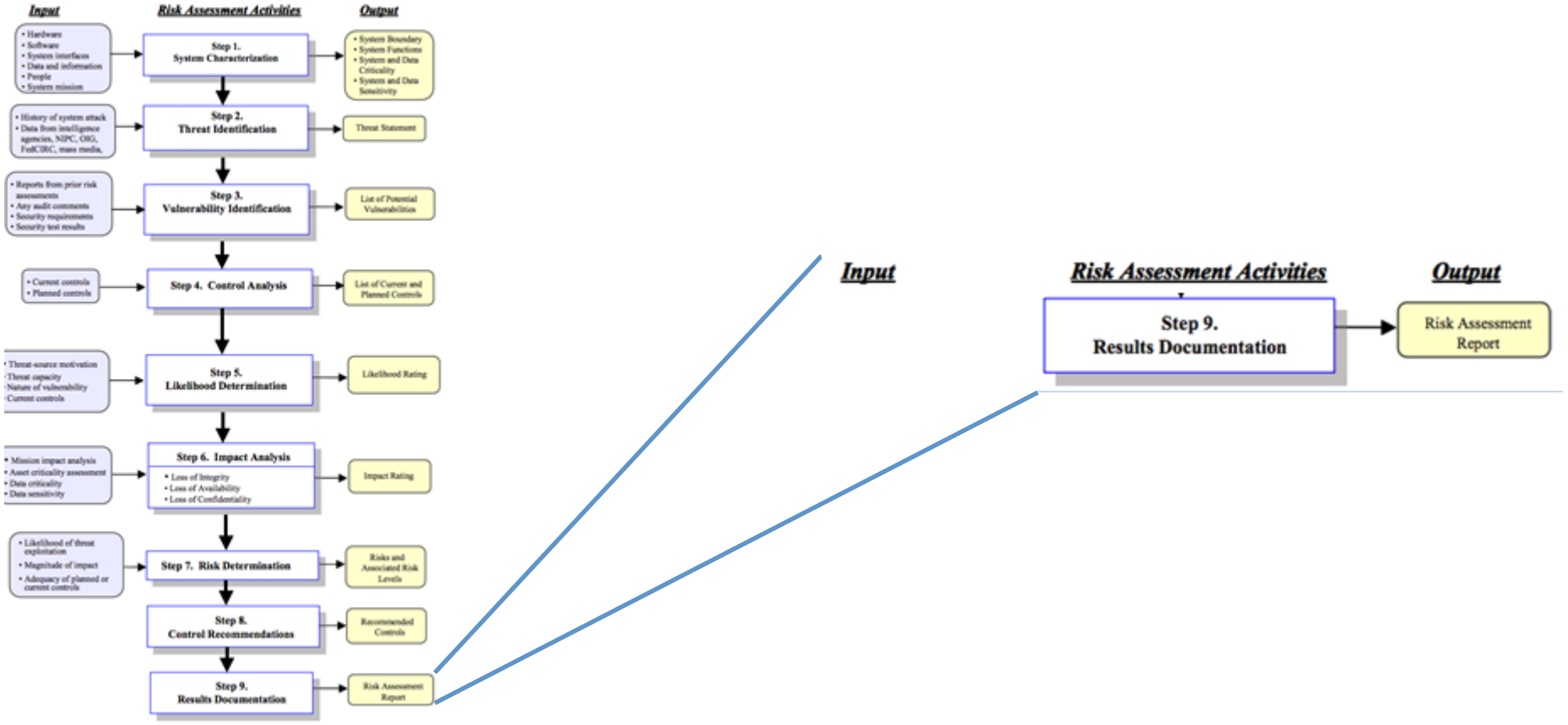
Recommending Controls: Or, What to do about your Risks?

- Accept: Do nothing. Cure may be worse than the disease.
- Avoid: Get rid of risk but turning off service or getting rid of asset (e.g. don't keep user info).
- Limit: Reduce impact by improved controls to prevent, detect or respond.
- Transfer: Find someone else to take the risk (usually paying them to do so).

Factors to consider in risk mitigation...

- Risk level (impact, likelihood).
- Cost to mitigate (dollars, staff time).
- How long will it take to mitigate?
- How effective will the mitigating controls be?
- How will controls impact usability?
- Can a single control benefit multiple risks (e.g. backups, firewall, intrusion detection)?

Step 9: Results Documentation



Why document?

Make long-term management easier since re-evaluation builds on previous assessment.

Communicates not only your program, but the motivations for it.

Allows you to demonstrate not only your program but the depth of thinking to others - builds trust in your project.

Re-evaluation over the long-term

Do regularly.

- Annually common.

Re-assess your assets, threats, and likelihoods:

- Changes from experience.
- Changes to project.
- Changes in threat landscape.

Have tolerances for risks changed?

Review controls

- Procedures being followed or are they too cumbersome?
- Do training and policies need updating?

What did you learn from any incidents?

CASE STUDY:
CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

CTSC

The mission of CTSC is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors.

This mission is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community.

Cybersecurity program available at:
http://trustedci.org/cybersecurity-program/

CTSC Cybersecurity Plan Steps

- System Characterization
- Identify Threats
- Risk/Threat Assessment
- CTSC Cybersecurity Policies and Procedures

Step 1) What are we trying to protect?

System Characterization: Process of defining the project environment including infrastructure, workflows, key assets and resources.

CTSC System Characterization

Define our workflows and activities:

- Collaborative engagements,
- Development of educational materials,
- Development of practices for CI cybersecurity,
- Fostering research to practice,
- Organizing workshops, training, Cybersecurity Summit,
- Dissemination of information: www.trustedci.org.

CTSC System Characterization

Define our staff demographics:

Roughly 10 FTEs consisting of staff from :

- Pittsburgh Supercomputing Center (PSC),
- Indiana University (IU) ,
- University of Illinois Urbana-Champaign (UIUC),
- University of Wisconsin (UW),
- University of Wisconsin-Milwaukee (UW-M).

CTSC System Characterization

What Infrastructure are we responsible for?

- Google Drive for storage of documents related to engagements, practices under development, meeting notes and operation of the project.
- GoDaddy for management of trustedci.org domain and DNS.
- SquareSpace for hosting of trustedci.org website.
- Blogger for hosting of blog.trustedci.org.
- Twitter account for public dissemination.
- IU systems for email lists and conference calls.
- Staff's local organization infrastructure for networking, computing, email, etc.
- Personal computing devices, cell phones, etc.

CTSC System Characterization

Who is our user community?

- NSF CI Community.

What are our organizational relationships?

- Staff institutions (CMU, IU, UIUC, UW, UWM) providers of basic infrastructure, cybersecurity and policies by which those staff abide.
- Commercial companies, contracted: GoDaddy and SquareSpace are contracted by CTSC for domain and web hosting.
- Commercial companies, non-contracted: Blogger and Twitter.

CTSC System Characterization

What are our key assets?

- **Sensitive information**: While CTSC does not handle any formally classified information, it may handle information from collaborators that is private by request of those collaborators or deemed sensitive by CTSC.
- **Private information**: Data from collaborations and normal business it may have information that is not intended to be public.
- **Public Communications**: CTSC operates a website, blog and Twitter feed. Compromise of these assets would be embarrassing to CTSC as a cybersecurity organization. Integrity of these assets is very important.

Step 2) What are our threats?

Start by identifying threats against our key assets. We used a visual diagram to show the relationship between threats and assets "Attack Trees."

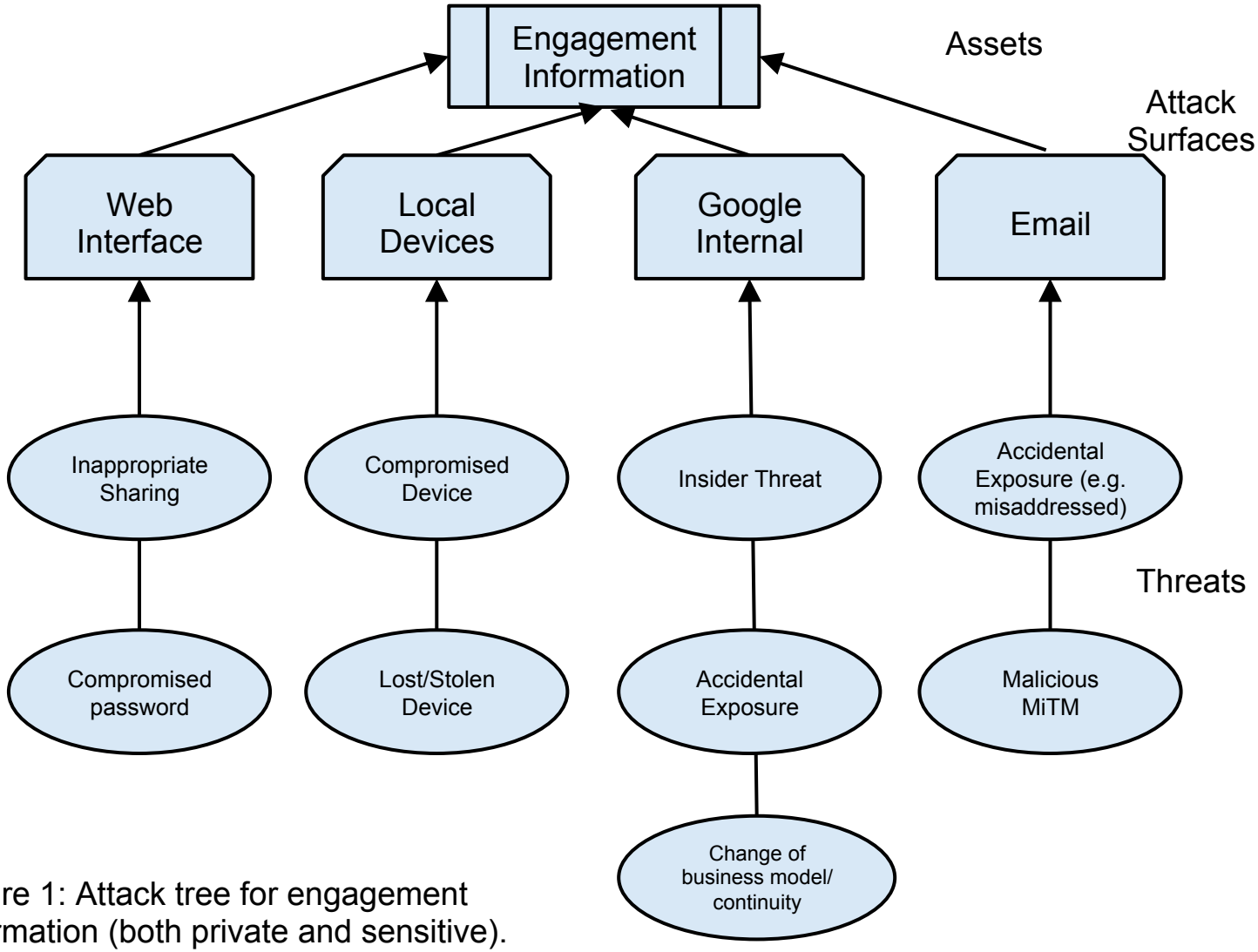


Figure 1: Attack tree for engagement information (both private and sensitive).

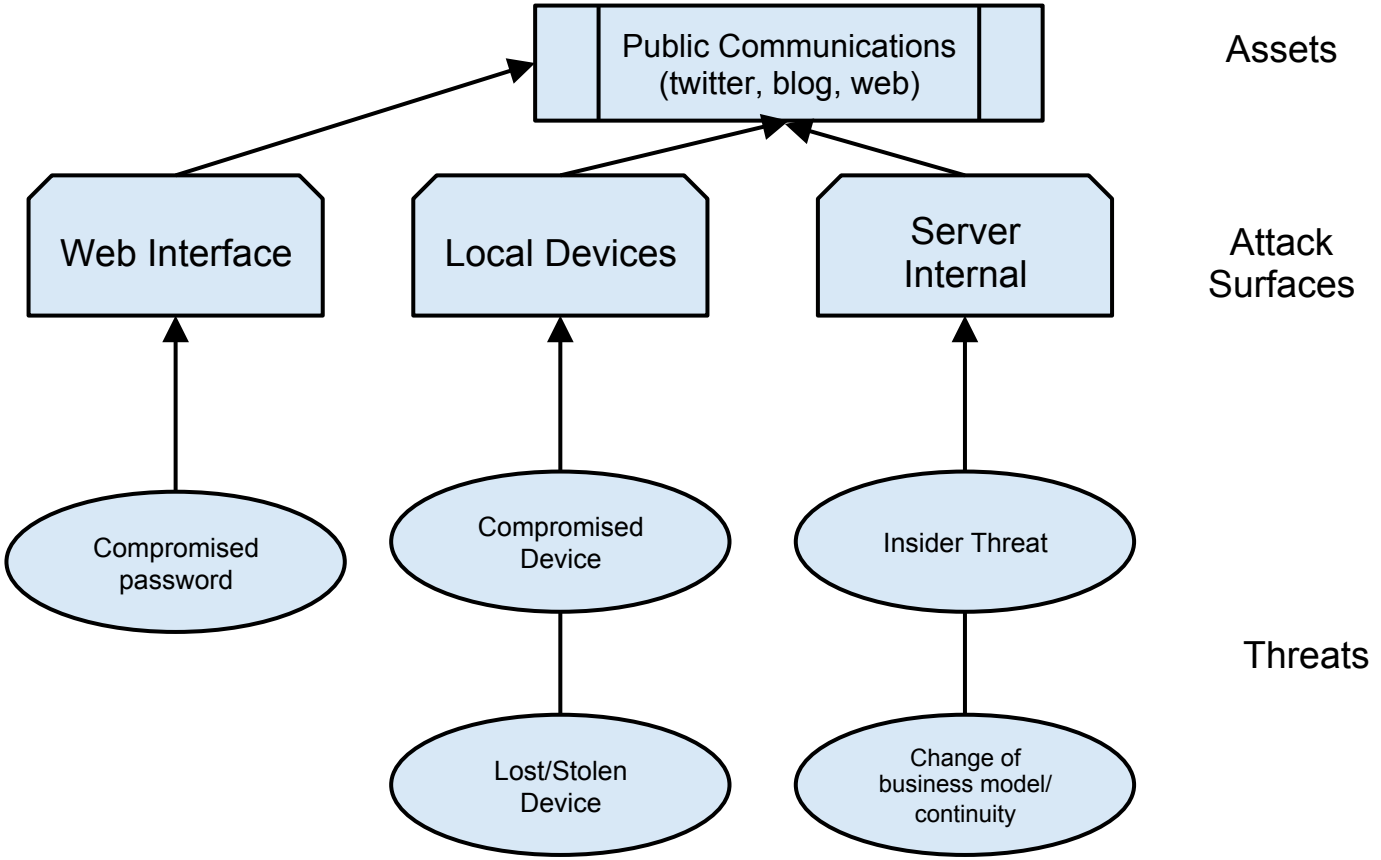


Figure 2: Attack tree for public communications information.

Step 3) Threat Assessment and Risk Mitigation

For each threat consider:

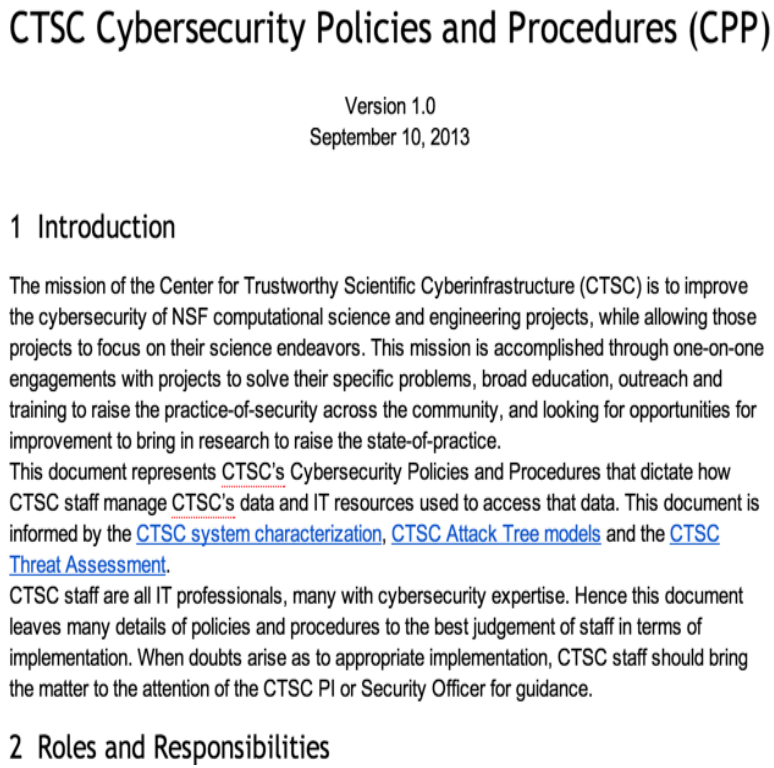
- What would the impact be to the project?
- What is the likelihood it could occur?
- How can we reduce the risk?

CTSC Threat Assessment Version 1.0 August 20, 2013

Asset	Sensitivitiy/Impact - Asset CIA Requirements - Value	Surface	Threats	Impact	Likelihood	Mitigations in Place	Possible Additional Mitigations	Evaluation	Notes
Engagement Information (Private and Sensitive)	Sensitive: C,I - High; Private: I - High, C - Medium; Both: A - Low	Google Drive Web Interface	Inappropriate Sharing	C, I	Low-Medium	None today	Sharing Policy, Audits of Sharing	Implement Possible Mitigations	Accidential sharing of document with public or inappropriate personnel.
			Compromised Password	C, I	Low	None today	Policy on password strength and (non-)reuse, require Google 2-factor for CTSC staff.	Implement Possible Mitigations	
		Local Device	Compromised Device	C, I	Low	Local IT policies on securing devices	None	No reasonable course of action, accept risk.	Device may contain copies of documents and/or allow access to web interface via open session or cached password.
			Lost/stolen Device	C, I	Low	None today	Policy on lost devices	Implement Possible Mitigations	
		Google Internal	Insider Threat	C, I	Low	None today	Encryption	Implemnent encryption for Sensitive Information	
			Accidential Exposure	C, I	Low	None today	Google alerts for public appearance, Encryption	Implement alerts and require encryption for Sensitive Information	
			Change of business model/continuity	A	Low	Copies of documents on local devices via Google sync	None	No reasonable course of action, accept risk.	Would persumably have time to shift to alternative.
		Email	Accidential Exposure	C, I	Low	None today	Encryption	Require encryption for Sensitive Information	Engagement information in email
			Malicious MiTM	C, I	Low	None today	Encryption	Require encryption for Sensitive Information	

CTSC Cybersecurity Policies and Procedures

- Roles and Responsibilities.
- Data handling and access policy.
- Data classification guidelines.
- Staff device management.
- Guidelines for public facing services (website, twitter).
- Incident response plan.



CTSC Cybersecurity Policies and Procedures (CPP)

Version 1.0
September 10, 2013

1 Introduction

The mission of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) is to improve the cybersecurity of NSF computational science and engineering projects, while allowing those projects to focus on their science endeavors. This mission is accomplished through one-on-one engagements with projects to solve their specific problems, broad education, outreach and training to raise the practice-of-security across the community, and looking for opportunities for improvement to bring in research to raise the state-of-practice.

This document represents CTSC's Cybersecurity Policies and Procedures that dictate how CTSC staff manage CTSC's data and IT resources used to access that data. This document is informed by the CTSC system characterization, CTSC Attack Tree models and the CTSC Threat Assessment.

CTSC staff are all IT professionals, many with cybersecurity expertise. Hence this document leaves many details of policies and procedures to the best judgement of staff in terms of implementation. When doubts arise as to appropriate implementation, CTSC staff should bring the matter to the attention of the CTSC PI or Security Officer for guidance.

2 Roles and Responsibilities

HOW TO EVALUATE A CYBERSECURITY PLAN

How to judge a cybersecurity plan…
(without becoming a cybersecurity expert)

You are a PI and a cybersecurity plan is being presented to you. What should you be looking for?

Your cybersecurity plan has been in place for a year, is it working well?

Some things to consider...

Big Picture Considerations

Is the plan comprehensible?

- Length and complexity is not good for its own sake.
- Does it have goals and metrics, or is it all details?

Does it have buy-in from other key leadership and stakeholders? Do you believe in it?

Does it capture the key assets of your project that are important to you?

Are the accepted risks OK with you?

Is it clear what everyone's roles and responsibilities are?

Does it leverage, or at least mesh well with, existing organization cybersecurity services and policies?

Information Security Responsibilities as listed in the Cooperative Agreement

The NSF CA language is a good (or required) checklist of topics to have:

- Roles and responsibilities, risk assessment, technical safeguards, administrative safeguards; physical safeguards; policies and procedures; awareness and training; notification procedures.
- Evaluation criteria employed to assess the success of the program.

Balance

Does it address preventative, detective and responsive controls, or does it focus too much on just one?

Does it cover technical, policy and educational controls?

Is usability considered? Does it show a good understanding of your user community needs for security and usability?

Every rule has exceptions - is it clear (and OK with you) who gets to make exceptions to the policy?

Over time…

Is the plan being followed?

Has it established trusted relationships you need?

Is the plan regularly reviewed and updated?

Are key project milestones handled?

- E.g. going to production, serving a new user community.

Incidents….

- Did everyone know their role?
- Was there good communication?
- Was there a post mortems and lessons learned?

WRAP UP

Acknowledgements

Training built on experiences of the
CTSC Team and developed by

Patrick Duda, James Marsteller, Randy Butler,
Rakesh Bobba, Von Welch and Craig Jackson.

This material is based in part on work supported by the National Science Foundation under Grant Number OCI-1234408. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Thank you

Please complete an evaluation of this training at

http://go.iu.edu/8r6

Slides available at trustedci.org/training

ADVANCED CYBERSECURITY PROGRAM

What might an advanced cybersecurity program look like?

What does “advanced cybersecurity program” mean?

- A mature program refined over time.
- A program with defined resources.
  - Committed funds for security budgeted.
    - Technical controls.
    - Training/education program for staff.
  - Dedicated security staff.
- A project with above average security requirements.

What might an advanced cybersecurity program look like?

Might include more complex technology:

- Intrusion detection and prevention systems.
- Automated vulnerability scanning.
- Advanced network access control.
- Defence in depth techniques.
  - Host and network strategies.

What might an advanced cybersecurity program look like?

Processes, Policy and Accounting:

- External audits to verify policy compliance.
- Red team penetration testing.
- Robust contingency plans and/or testing.
- Detailed accounting and analysis.
- Strong participation in security communities.
- Mandatory training requirements.

What might an advanced cybersecurity program look like?

Well-defined metrics for success with regular assessment.

Regular reviews by outside parties (e.g. peer projects, CTSC).

Thank you

Please complete an evaluation of this training at

http://go.iu.edu/8r6

Slides available at trustedci.org/training